ergonomic solutions

Come proteggere dispositivi, dati e reti

PCI DSS 3.0 compliance e che cosa questo significa per voi

Un libro bianco di Ergonomic Solutions
Prefazione di Chris Field della Fieldworks Connections

TECHNOLOGY MOUNTING SOLUTIONS

Perché la sicurezza dei pagamenti in-store non si limita a lucchetti e chiavi

Nonostante l'avvento sia di una regolamentazione sia delle migliori pratiche in Europa per migliorare la sicurezza dei pagamenti, c'è ancora molta incertezza, da territorio a territorio, sulle modalità con cui i commercianti debbano raccogliere questa sfida.

Per alcuni, l'incertezza è stata sfruttata da fornitori che usano la paura per costringere i commercianti ad adottare misure che sono a volte eccessive, con il risultato di investimenti inutili, una scarsa ergonomia nel punto vendita e difficoltà per i consumatori che utilizzano i dispositivi di pagamento.

Talvolta, le misure adottate vanno nella direzione sbagliata, per esempio, se da un lato può apparire che soddisfino i requisiti delle linee guida del PCI Council, possono non funzionare in tutte le circostanze in un ambiente reale.

Resta il semplice fatto che, se da un lato la maggior parte degli aspetti degli standard PCI sono stati presi in considerazione dai produttori di terminali, l'ultima linea di difesa nei confronti dei potenziali criminali rimane sulle spalle del retailer. E questi criminali stanno diventando più intelligenti e più determinati da un giorno all'altro: ogni giorno, sono oltre 5.000 i terminali disponibili per le aste online, e i terminali legittimi nei negozi sono costantemente in pericolo.

Di conseguenza, i retailer sono inondati da società operanti nel settore della sicurezza dei dispositivi di pagamento, in parte a causa dei requisiti loro imposti dal settore delle carte di pagamento, ma anche perché il problema della sicurezza dei dati continua a far notizia e ad aumentare le preoccupazioni dei consumatori.

Si tratta di preoccupazioni reali, evidenziate dall'impatto che pratiche negligenti di protezione dei dati possono avere sui retailer di qualsiasi dimensione; tuttavia la pressione esercitata sui retailer affinché reagiscano a tali sfide arriva proprio in un momento in cui sono costretti a prestare attenzione come mai prima d'ora ad ogni singolo investimento. Dovendo già operare in un ambiente difficile, i retailer sono costretti a concentrarsi maggiormente sull'esperienza del cliente, e con nuovi investimenti in dispositivi mobili che si connettono alla rete wireless e che tuttavia devono anche soddisfare i requisiti PCI DSS 3.0 per la protezione dei dati.

Abbiamo deciso di lavorare con il leader del mercato, Ergonomic Solutions, su richiesta dei nostri retailer associati per portare un po' di buon senso nel problema, pubblicando una guida sulle migliori pratiche sulla sicurezza dei dati di pagamento che abbraccia non solo la sicurezza fisica dei terminali e degli altri dispositivi di pagamento, ma anche le implicazioni della PCI compliance sulla sicurezza, gestione, registrazione e manutenzione dei dispositivi, come pure sull'ambiente di pagamento.

La nostra missione è quella di analizzare il problema in modo imparziale e aiutare i commercianti a capire le loro possibilità di scelta in modo che possano prendere decisioni in base alle loro esigenze specifiche.

Utilizzando questa guida, i commercianti potranno con maggiore facilità rispettare pienamente le raccomandazioni PCI DSS 3.0 su:

- sicurezza fisica dei terminali di pagamento
- ambiente dei pagamenti
- prevenzione della strisciata
- valutazioni del rischio

Questo approccio è sostenuto dalle primarie organizzazioni in materia di pagamenti, da VeriFone a Visa e segue le linee guida e i requisiti pubblicati dal PCI Council.

Chris Field
Fieldworks Connections

Le minacce

Qualcuno nel settore dei pagamenti ha voluto incutere paura per spingere i commercianti lungo l'irto percorso di una sicurezza a volte eccessiva, a volte errata e, altre volte, inutile dei dispositivi fissi e mobili in-store e altri componenti aggiuntivi per il punto vendita.

Significativi investimenti vengono operati nei terminali di pagamento, per cui l'ultima cosa di cui numerosi retailer vogliono sentir parlare è che debbano spendere ancora più soldi sulla sicurezza dei dispositivi. L'approccio onesto consiste nell'aiutarli a comprendere i rischi e creare un proprio profilo di rischio sulla cui base operare qualsiasi successivo investimento. Ciò contrasta nettamente con gli spacciatori di paura unicamente interessati a vendere apparecchiature.

Occorre quindi raggiungere un compromesso tra inerzia e reazione eccessiva.

La PCI DSS 3.0, 9.9 afferma che un esercente deve proteggere da manomissioni e sostituzioni i dispositivi POS (point-of-sale) che acquisiscono dati delle carte di pagamento attraverso l'interazione fisica diretta con la carta. ***Diventerà un obbligo per i dettaglianti a partire dal 30 giugno 2015****.*

Per i dispositivi mobili la guida asserisce che laddove un esercente possiede o è in altro modo responsabile di un dispositivo mobile utilizzato nell'ambito di una soluzione di pagamento, spetta all'esercente adottare misure per consolidare e mantenere la sicurezza del dispositivo. Le misure descritte in questa sezione devono essere applicate anche ad eventuali componenti hardware aggiuntivi che fanno parte della soluzione mobile di accettazione dei pagamenti (ad es. lettori di schede).

5.1. Impedire accessi non autorizzati al dispositivo fisico

5.1.1. Il dettagliante è tenuto ad assicurare l'integrità e la sicurezza del dispositivo mobile e la sua conservazione in luogo sicuro quando non è in uso (ad es. chiudendolo a chiave in un armadietto, ancorandolo a un banco o tenendolo sotto sorveglianza 24 ore al giorno).

Le minacce sono reali e l'obbligo di ridurle ai sensi dei Payment Council Industry Data Security Standard (PCI: DSS) è fondamentale se i retailer vogliono evitare multe e una perdita di fiducia dei clienti se i dati vengono rubati.

Qualsiasi violazione della sicurezza dei dati delle carte di pagamento ha conseguenze di vasta portata sulle organizzazioni coinvolte, tra cui:

- obblighi normativi di segnalazione
- perdita di reputazione
- perdita di clienti
- potenziali passività finanziarie
- contenzioso

PARTICIPATING ORGANIZATION

Tuttavia, numerosi produttori di dispositivi di protezione fisica semplicemente ignorano la PCI e si concentrano solo sul dispositivo.

Ne derivano:

» investimenti errati
» mancanza di redditività a lungo termine
» mancata PCI compliance
» il dispositivo selezionato diviene obsoleto molto prima di arrivare al ritorno dell'investimento
» il dispositivo selezionato agisce da deterrente per i truffatori, ma allontana anche i clienti

La paura può tendere a superare gli istinti naturali dei retailer ad assicurarsi che tutti gli investimenti in tecnologia e apparecchiature siano supportati da un solido ritorno dell'investimento e da un modello di costo totale di gestione. Questo è sbagliato, poiché per acquistare i retailer non solo vogliono comprendere la concreta redditività finanziaria, ma anche benefici più intangibili ma comunque cruciali in termini di esperienza del cliente.

Occorre considerare pro e contro tra sicurezza, accessibilità e design. La soluzione deve tenere conto della situazione futura e non limitarsi a risolvere un problema e poi ad ammortizzare.

Non si tratta solo del dispositivo

Poiché gli standard PCI riguardano la protezione dei dati, è importante proteggere non solo il dispositivo ma tutto il cablaggio che lo collega alla rete, la rete a cui si appoggia e l'intero l'ambiente a cui si appoggiano la rete e i dispositivi. Trattando le apparecchiature indipendentemente dalla rete si corre il rischio di molteplici soluzioni fra loro incompatibili, di settori che possono passare inosservati, di una possibile duplicazione degli sforzi ed è possibile che un modello di ritorno dell'investimento non trovi facilmente conferma.

Concentrarsi sul solo dispositivo può comportare costi significativi:

» se il dispositivo non è fissato, può cadere durante il passaggio fra il personale e i clienti
» il cablaggio si usura con il rischio che il dispositivo passi alla modalità antisabotaggio divenendo di fatto inutilizzabile

» mettere in sicurezza il solo dispositivo non necessariamente dissuade da frodi su altre parti della rete, ad es. sui cavi

Dobbiamo quindi considerare due aspetti principali:

» mettere in sicurezza il dispositivo, sia fisso che mobile
» mettere in sicurezza l'ambiente

Requisiti PCI DSS 3.0 30 giugno 2015

Mettere in sicurezza il terminale o dispositivo mobile

Secondo Visa, i retailer dovrebbero tenere traccia e monitorare i dettagli di tutti i dispositivi di accettazione di pagamento che accettano le proprie carte. In questo contesto, i retailer dovrebbero controllare regolarmente che i dispositivi non presentino anomalie, quali sigilli o viti mancanti o alterati, fili estranei, fori nel dispositivo o l'aggiunta di etichette o altro materiale che potrebbe essere utilizzato per mascherare i danni arrecati da manomissioni. I retailer dovrebbero come minimo eseguire i seguenti controlli:

» il terminale si trova nella corretta ubicazione?
» è corretto il nome del fabbricante?
» è corretto il numero del modello?
» è corretto il numero di serie stampato sull'etichetta e visualizzato a schermo?
» il colore e le condizioni generali del terminale sono quelli descritti senza segni aggiuntivi o graffi (specialmente attorno ai giunti)?
» i sigilli di garanzia e le etichette del fabbricante sono presenti senza segni di tentativi di distacco o manomissione?
» i contrassegni di sicurezza e i numeri di riferimento del fabbricante sono quelli descritti?
» gli eventuali contrassegni ultravioletti sono quelli descritti?
» tutte le connessioni al terminale corrispondono a quanto descritto, utilizzano lo stesso tipo e colore dei cavi e non presentano fili allentati o connettori rotti?
» il numero delle connessioni in ingresso al terminale corrisponde a quello previsto?
» il numero totale di terminali in uso corrisponde al numero di terminali ufficialmente installati?

La messa in sicurezza del terminale ha i seguenti obiettivi:

» prevenire il furto o la sostituzione con un terminale non autorizzato
» prevenire l'acquisizione dei dati dall'infrastruttura di pagamento

» l’aggiunta di apparecchiature per la strisciata al terminale o rete
» proteggere i dati del PIN vulnerabili al shoulder surfing
» proteggere i terminali incustoditi e prevenire la rimozione fisica
» proteggere non solo il terminale, ma anche i cavi

Il diagramma descrive l’ecosistema di dispositivi di pagamento, le applicazioni, l’infrastruttura e la struttura di utenti e gli utenti strutturati dagli standard di sicurezza PCI.

Noi riteniamo che sia consigliabile trovare il giusto equilibrio tra proteggere il bene e pregiudicare la facilità d’utilizzo e, quindi, il servizio ai clienti. Un dispositivo può essere protetto in modo da renderne pressoché impossibile il furto, ma questo non scoraggia necessariamente un tecnico disonesto o un dipendente collusivo. Nel documento PCI dal titolo Skimming Prevention: Best Practices for Merchants, si raccomanda vivamente ai retailer la buona regola di utilizzare dei cavetti antifurto con servizi di gestione delle chiavi, nonché di ricorrere a sistemi di registrazione e monitoraggio per prevenire la compromissione sia dei terminali che dei cavi.

Si dovrebbe tuttavia tenere conto anche dell’ubicazione fisica del dispositivo e della sicurezza dei componenti. Può essere rimosso facilmente? I componenti sono collegati o fisicamente protetti per evitare la manomissione o il furto facili? I dispositivi devono essere sempre collocati in una ubicazione che consenta al cliente di utilizzarli in modo da oscurare l’immissione del PIN agli altri clienti e devono possibilmente includere uno schermo a protezione da sguardi indiscreti durante l’immissione del PIN.

L’usabilità non si limita alla sola praticità, ma include anche il rispetto della regolamentazione europea su disabilità e accessibilità. Se i requisiti normativi possono essere soddisfatti con il dispositivo fissato a un supporto di montaggio, occorre prendere in considerazione una modifica del supporto trasformandolo da un meccanismo “di solo supporto” a un meccanismo che trattiene fisicamente il dispositivo riducendo il rischio di un furto con strappo. Se il fissaggio del dispositivo al supporto di montaggio dovesse contravvenire alla normativa su disabilità e accessibilità, si prenderà in considerazione il collegamento di un cavetto antifurto al dispositivo e al supporto di montaggio in modo da consentire un certo grado di movimento, mantenendo tuttavia la sicurezza nei confronti di un furto con strappo.

Il crescente utilizzo di tecnologie orientate al cliente in ambiente retail attraverso dispositivi come terminali Chip & PIN, iPad, e una serie di altri dispositivi portatili può aver generato una nuova esperienza di acquisto per molti, ma il prezzo da pagare è stato un incremento di furti e frodi. Il negozio in generale e il punto vendita in particolare sono a rischio di forme di criminalità sempre più sofisticate. Gli aspetti maggiormente a rischio sono i dati delle carte e le informazioni PIN . Dall'esperienza risulta che ci vogliono solamente circa 30 secondi per rimuovere un intero dispositivo di accettazione della carta e sostituirlo con uno identico dotato di skimmer elettronici.

I criminali hanno sviluppato una conoscenza approfondita della funzionalità e delle vulnerabilità di numerosi terminali. Una volta superate le protezioni di un particolare terminale, diventa più facile utilizzare queste informazioni per attaccare terminali analoghi, rendendo la sicurezza dei punti vendita ancor di attualità.making POS security all the more relevant.
L'iPad e altri tablet hanno trasformato il modo in cui utilizziamo la tecnologia mobile e hanno ingenerato una rivisitazione del tradizionale approccio all'integrazione della tecnologia commerciale, specialmente in seno al settore retail. Ma questi dispositivi hanno un valore elevato e sono molto ricercati.

Per proteggere le informazioni digitali, prevenire la perdita dei dati e proteggere ulteriormente l'hardware, Ergonomic Solutions dispone di una gamma di lucchetti di sicurezza per terminali di pagamento, dispositivi mobili e hardware POS.

Mettere in sicurezza l'ambiente

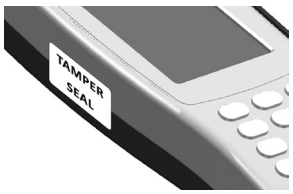
Si tratta in questo caso di mettere in sicurezza il dispositivo in quanto dispositivo connesso con IP. Ora che i dati sono crittografati point to point, lungo l'intera rete, tutti i punti di vulnerabilità devono essere verificati e messi in sicurezza e devono essere attuati processi e procedure per il loro monitoraggio.

- Registrazione e monitoraggio dei dispositivi
- Compliance di processi e procedure
- Documentazione delle migliori prassi
- Valutazione dei rischi
- Analisi dell'impatto e procedure di intervento

Registrazione e monitoraggio dei dispositivi

Mettere in sicurezza i dispositivi è una cosa, ma è perfettamente possibile che il dispositivo sicuro sia stato compromesso e non siano state predisposte delle procedure per individuare questo problema. Con l'incremento dello skimming, che vede i truffatori manomettere i dispositivi nel tentativo di rubare i dati delle carte attraverso sia il dispositivo che la rete, è fondamentale registrare tutti i dispositivi, un aspetto che va incontro alle raccomandazioni del PCI Council.

La registrazione deve includere le seguenti caratteristiche chiave:



- numero di serie del dispositivo e numero del modello
- fabbricante
- segni particolari esistenti (derivanti dall'usura)
- immagine del dispositivo
- tipo di connessione
- colore del cavo
- numero di connessioni
- espositori, scatole per beneficenza o altro materiale di merchandising nella vicinanza del terminale
- ubicazione di sigilli di sicurezza (sigilli di fabbricazione o sigilli supplementari)
- ubicazione nel sito, ad es. numero di cassa 1

I terminali manomessi possono quindi essere identificati essendo state registrate le loro caratteristiche originali univoche. Se il terminale presente differisce in qualsiasi modo, esiste il rischio di frode.

In questo modo, la sicurezza per l'utente è maggiore in quanto i terminali sono dotati di un account univoco ed è anche più intelligente per un'organizzazione che vuole assicurarsi che le proprie apparecchiature siano registrate e utilizzabili anche in caso di cambiamento di personale.

La registrazione consente inoltre agli amministratori di gestire i programmi di blocco attraverso un unico portale web, e di gestire l'accesso e le chiavi in modo personalizzato per il singolo ambiente, assegnando le chiavi a una persona, una cassa, una regione a seconda dei casi.

Gli amministratori possono

- registrare lucchetti individualmente o in massa a singoli individui o a gruppi (negozi/aree, ecc.)
- gestire programmi con chiavi master tipo passepartout, chiavi uguali o condivise
- creare account utente per gli utenti finali su cui sia possibile ordinare chiavi di ricambio o salvare i codici di combinazione
- suggerire agli utenti di accedere ad esercitazioni video e validare i dettagli dell'account
- registrare la proprietà dei lucchetti e scaricare i rapporti
- trovare i proprietari delle chiavi smarrite
- riassegnare i lucchetti ai nuovi utenti

Gli individui possono:

» ordinare chiavi sostitutive
» recuperare codici di combinazione salvati (forse per il futuro?)
» convalidare dettagli di account e codici
» aggiornare i propri dati personali

Noi raccomandiamo altresì un sistema di marcatura unico dei dispositivi per una ulteriore protezione contro le manomissioni, quali sigilli olografici visibili solo alla luce UV e che, se manomessi, ne rendono impossibile la sostituzione o riparazione. Un sigillo non è solo a prova di manomissione, ma segnala anche al personale che il terminale di pagamento è un dispositivo POS che deve essere trattato con cura e con particolari procedure al fine di soddisfare le norme di sicurezza.

Allineamento

L'approccio consigliato in questo rapporto è convalidato dal documento del PCI DSS 3.0 Council: Point-to-Point Encryption. Solution Requirements and Testing Procedures: Encryption, Decryption, and Key Management within Secure Cryptographic Devices, Versione 1.1.1.

3A-1.1 Mantenere in essere procedure di controllo e monitoraggio delle scorte al fine di identificare e individuare tutti i dispositivi POI (point-of-interaction), compresi i punti in cui si trovano i dispositivi:

- installati
- in attesa di installazione
- in corso di riparazione o comunque non in uso
- in transito

Soluzione: registrare e recuperare database e checklist

3A-1.2 Eseguire gli inventari dei dispositivi POI almeno una volta all'anno per rilevare la rimozione o sostituzione dei dispositivi.

Soluzione: registrare e recuperare le checklist

3A-1.3 Mantenere un inventario documentato di tutti i dispositivi POI includendo almeno i seguenti:

- marca, modello del dispositivo
- ubicazione (sito/struttura, e/o identità del commerciante)
- numero di serie
- descrizione generale
- fotografia del dispositivo che mostra chiaramente il tipo di dispositivo e il modello (per agevolare l'identificazione di dispositivi diversi)
- sigilli di sicurezza, etichette, marcature nascoste, ecc.
- numero e tipo di connessioni fisiche al dispositivo
- data dell'ultimo inventario eseguito
- versione firmware
- versione hardware
- applicazioni (versioni incluse)

Soluzione: registrare e recuperare database

3A-1.4 Applicare le procedure per individuare e rispondere alle variazioni nell'inventario annuale, compresi i dispositivi POI mancanti o sostituiti. Le procedure di intervento devono includere tutte le eventuali procedure definite da parte di tutti i marchi di pagamento PCI applicabili, compresi i termini per la notifica degli incidenti e la predisposizione di un punto di contatto cui i commercianti possano rivolgersi per segnalare i dispositivi mancanti/sostituiti.

Soluzione: registrare e recuperare il database

3A-4.1 Fornire istruzioni tramite il manuale di istruzioni P2PE sulla selezione, da parte del commerciante, di ubicazioni appropriate per i dispositivi installati, ad esempio:

- Controllare l'accesso del pubblico ai dispositivi in modo tale che sia limitato solo ad alcune parti del dispositivo che una persona utilizza normalmente per espletare una transazione (ad esempio, tastierino mobile PIN e lettore di carte).
- Posizionare i dispositivi in modo che possano essere osservati e/o monitorati dal personale autorizzato (per esempio, durante i controlli quotidiani dei dispositivi eseguiti dagli addetti del negozio/alla sicurezza).
- Posizionare i dispositivi in un ambiente che scoraggi i tentativi di violazione (per esempio, attraverso l'uso di un'illuminazione adeguata, percorsi di accesso, misure di sicurezza visibili, ecc.)

Soluzione: registrare e recuperare la checklist

3A-4.2 Fornire istruzioni tramite il manuale di istruzioni P2PE sulla cui base il commerciante possa proteggere fisicamente i dispositivi installati in modo da evitare la rimozione o la sostituzione non autorizzate, con esempi di come i dispositivi possono essere protetti fisicamente.

Soluzione: Registrare e recuperare
Cavetti antifurto

3B-8 Il fornitore di soluzioni implementa meccanismi di rilevamento di manomissioni per i dispositivi in possesso dei commercianti, e fornisce loro istruzioni correlate.

Soluzione: StealthSafe

3B-8.1.1 Fornire istruzioni tramite il manuale di istruzioni P2PE sulla cui base il commerciante possa eseguire controlli fisici periodici dei dispositivi per rilevare la manomissione o la modifica degli stessi. Le procedure dettagliate per l'esecuzione di controlli fisici periodici devono includere:

- descrizione dei meccanismi di rilevamento delle manomissioni
- linee guida per i controlli fisici, comprese fotografie o disegni del dispositivo che illustrano ciò che il commerciante deve controllare, ad esempio:

- sigilli o viti mancanti o alterati, cablaggi estranei, fori nel dispositivo, o l'aggiunta di etichette o altro materiale di copertura che possa essere utilizzato per mascherare i danni da manomissione del dispositivo.
- istruzioni sulla pesatura dei dispositivi POI al ricevimento e poi periodicamente, per un confronto con le specifiche del fornitore al fine di identificare l'eventuale inserimento di meccanismi di intercettazione nei dispositivi

- raccomandazioni sulla frequenza dei controlli

Soluzione: registrare e recuperare database e checklist
Cavetti antifurto

3B-8.2 Implementare meccanismi di rilevamento di manomissioni e/o processi per dispositivi installati in luoghi remoti o incustoditi; per esempio, utilizzare telecamere o altri meccanismi fisici per allertare il personale in caso di violazione fisica.

Soluzione: Cavetti antifurto

Informazioni su Ergonomic Solutions

Fondata nel 1996, Ergonomic Solutions è cresciuta rapidamente diventando leader mondiale nella progettazione, produzione e fornitura delle soluzioni di installazione e sicurezza più avanzate sotto il profilo ergonomico per una vasta gamma di tecnologia in-store e mobile per i mercati, ad es. retail, attività bancarie, trasporti pubblici e turismo. Ergonomic Solutions è da tempo all'avanguardia nella progettazione e ottimizzazione degli spazi di lavoro e la nostra Consulenza in Ergonomia ha insegnato a numerosi principali retailer europei come creare uno spazio di lavoro che ottimizza l'accessibilità, l'utilizzabilità, la sicurezza e il comfort del loro personale e dei clienti.

La nostra suite di prodotti tecnologici brevettati SpacePole®, Telehook®, ClickSafe® e Safe-Guard™ sono progettati ergonomicamente per permettere la flessibilità dei movimenti con possibilità di rotazione, inclinazione e regolazione del gomito e dell'altezza. Dalla fabbrica alle stanze del management, siamo in grado di fornire una soluzione che permette al vostro investimento IT di fare il miglior uso possibile dello spazio di lavoro disponibile, proteggendolo al tempo stesso da eventuali danni e furti.

Informazioni su Fieldworks Connections

Fieldworks Connections riunisce retailer, marchi e influencer per progettare il futuro del commercio multicanale.

Oggi facciamo parte di una comunità che abbraccia canali sia tradizionali che nuovi, in Europa, Asia e Stati Uniti. La nostra influenza ci consente di sostenere le aziende in cerca di crescita sui mercati da loro scelti e di ridurre il rischio mediante l'applicazione delle migliori pratiche.

Fieldworks Connections è guidata da un team di giornalisti esperti, operatori di marketing, analisti e consulenti, supportati da un consiglio di retailer, consulenti e studiosi di primo piano.

www.fieldworksconnections.co.uk